MBRCC Mortgage Broker Regulators' Council of Canada
CCARCH Conseil canadien des autorités de réglementation des courtiers hypothécaires

Mortgage Broker Regulators' Council of Canada (MBRCC)

Principles for Cybersecurity Preparedness

Purpose

The MBRCC is a forum for Canadian mortgage brokering regulators to collaborate and promote greater regulatory consistency to serve the public interest.

The purpose of this guidance is to support cybersecurity preparedness in the mortgage brokering sector by proposing practices to avoid cybersecurity incidents and properly respond to them when they occur.

Cyber threats are a growing risk for everyone, including the mortgage brokering sector. Managing this risk proactively helps protect against attacks seeking to compromise or steal electronic information.

Cybersecurity is the application of technologies, processes, and controls to defend infrastructure such as systems, networks, programs, devices, and data. It aims to reduce the likelihood and impact of cyberattacks that could lead to unauthorized access to sensitive client information and the disruption of business activities due to interference in critical infrastructure and corporate networks.

This guidance supports the Security and Confidentiality Principle (Principle 8) of the MBRCC Code of Conduct. This Principle states that "regulated persons and entities must protect their clients' information. They must use and disclose it only for purposes for which the client has given consent or as compelled by law."

Federal and provincial legislative frameworks require the protection of personal information. At the federal level, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) requires all businesses, including mortgage brokerages and administrators, to protect specific personal client information. For example, collected personal data must be protected from loss, unauthorized access and data theft.

This guidance does not create new obligations. MBRCC considers this guidance to be aligned with, and therefore can be interpreted in a manner consistent with, all existing requirements, rules, and standards of conduct.

Approach

This guidance provides four Principles describing the outcomes that regulated entities should achieve to ensure cybersecurity preparedness. It does not prescribe the way the Principles must be achieved. This principles-based approach offers regulated entities the flexibility to achieve the outcomes in a manner that is suitable for the size and structure of their business.

The guidance includes a checklist in Appendix A to help entities self-assess their cybersecurity preparedness. Appendix B lists leading cybersecurity standards that MBRCC referenced while developing these Principles.

Principles for Cybersecurity Preparedness

The common principles for mortgage brokering cybersecurity preparedness are:

1. Responsibility and Resourcing

Regulated entities should appoint a person responsible for overseeing cybersecurity risk to ensure accountability. Responsibility for complying with safe cybersecurity practices applies to all people in an organization, even if they do not have oversight roles. Entities should invest and assign all the resources needed to develop and maintain effective cybersecurity safeguards to protect client information, particularly personal information.

Regulated entities should:

- Develop cybersecurity preparedness policies and procedures.
- Require that individuals responsible for overseeing cybersecurity maintain their skillset and understanding of cybersecurity risks including ways to mitigate these risks through ongoing education.
- Raise awareness of cybersecurity risk by providing guidance to staff and management (as applicable) to ensure cybersecurity preparedness. This may include training and reminders of cybersecurity risks.
- Consider purchasing insurance for cybersecurity liability that is appropriate to their needs.

2. Identification and Prevention of Risks

Regulated entities should:

- Identify key cybersecurity risks like loss of client information or system access issues related to:
  - Access granted to staff;
  - Use of third-party service providers; and
  - Safeguarding of processes, technology hardware or facilities.
- Have appropriate "endpoint" risk detection protections, such as regularly updated anti-virus and malware scanning software.
- Conduct a cyber incident business impact assessment and ensure cybersecurity risks are part of the business continuity plan.
- Take adequate steps to minimize the likelihood and impact of a risk once identified.
- Determine the entity's comfort with identified risks ("risk tolerance").

Regulated entities are third-party service providers to financial institutions. Regulated entities should ensure that they understand and are compliant with a financial institution's expectations of third-party service providers regarding cybersecurity and, more broadly, information security.

3. Incident Monitoring, Detection and Response

Regulated entities should have a protocol for monitoring, detecting and responding to cybersecurity incidents as part of their policies and procedures for cybersecurity preparedness. The entity should have an incident response plan to protect client information and minimize service disruptions if an incident is detected. Aspects of this plan may include:

- Suspending some business processes to limit information vulnerability.
- Sharing relevant information about incidents with clients, third parties (including mortgage lenders) and regulators (as requested or, in some jurisdictions, required).
- Determining if the criteria for return to business as usual have been met.
- Restoring lost or corrupt data, processes and/or systems that would enable a return to business as usual.

4. Third-Party Management

Regulated entities are responsible for protecting their clients' information against cyber incidents by ensuring that their third-party service providers have cybersecurity preparedness practices in place. The mortgage brokering sector works within a network of providers; more complex and extensive networks increase cybersecurity risk. Careful relationship management is important to minimize vulnerabilities and to help ensure the protection of client information. Relationship management may include parties formally establishing processes and procedures for managing cybersecurity risks.

Appendix A – Cybersecurity Preparedness Checklist

Below is a basic cybersecurity[1] preparedness checklist. It may be useful for an entity without established cybersecurity preparedness practices.

This checklist is not comprehensive and does not cover all potential cybersecurity risks, However, it should help identify and address many of the basic risks related to mortgage brokering activities.

Any gaps/issues identified when going through the checklist should be prioritized based on the potential impact, likelihood of an incident and resources available. The gaps/issues should be addressed by a designated employee within a specific timeline.

☐ Do you have a person or people responsible for managing the organization's cybersecurity risks?

☐ Do you have an inventory of all computing devices used within the organization? For each device, document:

- Type of device (smart phone, tablet, desktop, laptop, server, etc.)
- Model number
- Serial number
- User responsible for the device
- Operating system and relevant applications installed on the device
- Whether the device is encrypted

☐ Do you have a list of all types of electronic records and data maintained on the organization's computer systems ("electronic assets") and where they are stored?

☐ Are electronic assets classified based on whether they contain any of the following:

- Personally identifiable information (PII)?
- Proprietary information?
- Sensitive financial information (for example, credit card information)?
- Transaction data?

☐ Have electronic records and data on the list that are important to the organization's ability to operate been identified?

☐ Has the backup and recovery process for electronic records and data been reviewed, updated and tested?

☐ Do you have policies and procedures to restrict and/or monitor the collection, storage, and use of sensitive client data?

☐ Has the information network been mapped for the organization (for example, how are computers and other computing devices connected? What servers/storage devices are on the network? How is the network connected to the internet, etc.?)?

☐ Has a risk assessment of computing devices, electronic assets and network topology been conducted by identifying:

- Which devices and assets are attractive attack targets?
- What attack vectors are there for gaining access to these devices and/or assets?
- Which actors may be seeking to attack the organization?
- What is the likelihood of a breach via a particular attack vector?
- What would be the impact of such a breach?
- How can the risk of a breach be reduced or perhaps eliminated?

---

[1] This checklist is based on Guidance released by the Financial and Consumer Services Commission of New Brunswick.

- ☐ Has a remote management tool been adopted to manage the organization's computing devices outside the organization's offices?
- ☐ Has a review of who has access to the organization's electronic assets been undertaken to ensure "least privilege"[2] access?
- ☐ Has cybersecurity awareness training been offered to employees, preferably on an ongoing basis?
- ☐ Have you reviewed or created key cybersecurity policies for the organization, including:
  - Cybersecurity best practices
    - Multi-factor authentication
    - Passwords
    - Clean desk
    - Using computing devices outside the office
  - Acceptable use of IT resources
  - New employee intake and exit
  - Acceptable use of personal devices for business purposes
  - Third parties and IT vendors
  - Has the organization's physical security been reviewed? Are the following controls in place to limit physical access to the organization's office(s)/building(s) to only the appropriate employees, including key card access, ID badges and visitor access rules?
- ☐ Does the organization have requirements for or agreements with independent contractors that address cybersecurity best practices?
- ☐ Does the organization verify that the disposal process for physical assets (old hardware, paper records, etc.) ensures all important records are properly destroyed or shredded at the end of life?
- ☐ Has the organization's network architecture been reviewed?
- ☐ Are proper firewall solutions, intrusion detection systems, server configurations and encryption mechanisms in place?
- ☐ Have the operating systems and network enabling applications been reviewed to ensure they are up to date and properly patched, and that an appropriate update schedule is in place and followed?
- ☐ Has up-to-date anti-virus/malware software been installed on all devices with access to electronic assets?
- ☐ Does your organization have proper insurance for cybersecurity liability?
- ☐ Has a cybersecurity breach incident response plan been established and tested?
- ☐ Has a business continuity plan and a disaster recovery plan been established and tested?

---

[2] An employee only has access to the information needed to do his or her work, and nothing more.

Appendix B – Other Cybersecurity Standards Examples

The MBRCC Principles for Cybersecurity Preparedness were developed by MBRCC regulators based on leading practices.

Referenced below are some of the resources referenced in developing this guidance

- International Organization of Standardization (ISO) - ISO/IEC 27001 — Information security management
- Cybersecurity Framework | National Institute of Standards and Technology
- Technology and Cyber Risk Management (osfi-bsif.gc.ca) – Office of the Superintendent of Financial Institutions